CLAIMS

What is claimed is:

1. An apparatus for managing access to a cryptographically secured access-controlled datum, comprising:

(a) input logic for receiving a candidate access code;

(b) a first memory configured to store a cryptographically camouflaged access-controlled datum;

(c) first cryptographic logic operatively connected to said input logic and said first memory for processing said cryptographically camouflaged access-controlled datum using said candidate access code; and

(d) output logic for providing said processed datum access-controlled datum to a user of said apparatus.

2. The apparatus of claim 1 wherein:

(a) said access-controlled datum has been at least partially encrypted using an access code;

(b) a second memory configured to store a cryptographic representation of said access code;

(c) said first cryptographic logic includes:

(i) second cryptographic logic operatively connected to said input logic and configured to regenerate said cryptographic representation of said access code in response to said candidate access code belonging to a plurality of pseudo-valid access codes; and

(ii) third cryptographic logic configured to receive said regenerated cryptographic representation from said second cryptographic logic, and operatively connected to said first memory and to said input logic for using said received candidate access code in

decrypting said stored encrypted access-controlled datum to produce a decrypted access-controlled datum.

3. The apparatus of claim 2 wherein said access-controlled datum is a cryptographic key.

4. The apparatus of claim 3 wherein said cryptographic key is a private key.

5. The apparatus of claim 4 further comprising a pseudo-public key corresponding to said private key.

6. The apparatus of claim 5 further comprising a pseudo-public certificate containing said pseudo-public key.

7. The apparatus of claim 6 wherein said pseudo-public key is encrypted.

8. The apparatus of claim 7 wherein said pseudo-public key is encrypted with a public key having a corresponding private key that is not generally known.

9. The apparatus of claim 4 wherein said private key is well-formed.

10. The apparatus of claim 9 wherein said private key includes a modulus not having any small factors, and an exponent smaller than said modulus.

11. The apparatus of claim 9 wherein said private key includes:

(a) a cleartext representation of said modulus; and

(b) a cryptographic representation of at least a part of an exponent corresponding to said modulus.

12. The apparatus of claim 11:

(a) further comprising a third memory for storing a number larger than said exponent and smaller than said modulus; and

(b) wherein said at least part of said exponent is stored in an expanded form which, when evaluated modulo said number, equals said at least part of said exponent.

13. The apparatus of claim 11 wherein said at least part of said exponent represents certain less significant bits of said exponent.

14. The apparatus of claim 3 wherein said second cryptographic logic for said regeneration of said cryptographic representation of said access code includes a many-to-one hash.

15. The apparatus of claim 14 wherein said many-to-one hash is a good hash.

16. The apparatus of claim 2 wherein:

(a) said cryptographic representation includes a hash function; and

(b) said second cryptographic logic for said regeneration of said cryptographic representation includes a many-to-one hash.

17. The apparatus of claim 16 wherein said many-to-one hash is a good hash.

18. The apparatus of claim 17 wherein said good hash is characterized in that said plurality of pseudo-valid access codes are distributed substantially uniformly among a plurality of invalid access codes.

19. The apparatus of claim 16 wherein said access-controlled datum is a private key.

20. The apparatus of claim 19 further comprising a pseudo-public key corresponding to said private key.

21. The apparatus of claim 19 wherein said private key is well-formed.

22. The apparatus of claim 19 further comprising digital signing logic including:

(a) input logic for receiving a message to be signed;

(b) randomizing logic for generating random data; and

(c) fourth cryptographic logic operatively connected to said input logic and to said randomizing logic for:

(i) padding said received message with said generated random data; and

(ii) signing said padded message with said decrypted access-controlled datum.

23. The apparatus of claim 2 wherein said third cryptographic logic is configured to disallow said decryption when said received candidate access code is an invalid access code.

24. The apparatus of claim 2 implemented as a software program.

25. The apparatus of claim 2 implemented as a hardware device.

26. The apparatus of claim 2 further comprising digital signing logic including:

(a) input logic for receiving a message to be signed;

(b) randomizing logic for generating random data; and

(c) fifth cryptographic logic operatively connected to said input logic and to said randomizing logic for:

(i) padding said received message with said generated random data; and

(ii) signing said padded message with said decrypted access-controlled datum.

27. The apparatus of claim 26 wherein said generated random data is strongly random.

28. The apparatus of claim 27 wherein said generated random data originates from a physical source.

29. The apparatus of claim 2 wherein said third cryptographic logic for decrypting includes a symmetric cryptographic function.

30. The apparatus of claim 29 wherein said symmetric cryptographic function is DES.

31. The apparatus of claim 1 wherein said stored access-controlled datum is a private key having a corresponding public key that includes a long exponent.

32. A cryptographic key wallet comprising:

(a) input logic for receiving a user-inputted access code that may belong to a plurality of pseudo-valid access codes;

(b) cryptographic logic for decrypting a stored access-controlled datum, using said pseudo-valid access code, upon cryptographically verifying said pseudo-valid access code; and

(c) output logic for providing said decrypted access-controlled datum to said user.

33. The cryptographic key wallet of claim 32 wherein said access-controlled datum includes a private key having a corresponding pseudo-public key.

34. The cryptographic key wallet of claim 33 further comprising a pseudo-public certificate containing said pseudo-public key.

35. A digital certificate server comprising:

(a) input logic for receiving from a requestor a digitally signed request for a pseudo-public digital certificate, said request including:

(i) a pseudo-public key to be certified, and

(ii) an identifying attribute of said requestor;

(b) cryptographic logic for verifying said digitally signed request using said pseudo-public key;

(c) logic for creating said pseudo-public certificate upon said verifying said digitally signed request, said certificate including a cryptographic representation of said pseudo-public key; and

(d) output logic for providing said pseudo-public certificate for said requestor.

36. The digital certificate server of claim 35 configured for use with a digital wallet, said digital wallet comprising:

(a) input logic for receiving a candidate access code;

(b) a first memory configured to store a cryptographically camouflaged access-controlled datum;

(c) first cryptographic logic operatively connected to said input logic and said first memory for processing said cryptographically camouflaged access-controlled datum using said candidate access code; and

(d) output logic for providing said processed datum access-controlled datum to a user of said apparatus.

37. The digital certificate server of claim 35 wherein said pseudo-public certificate is of a modified conventional format.

38. The digital certificate server of claim 35 wherein said pseudo-public key is encrypted.

39. The digital certificate server of claim 38 wherein said pseudo-public key is encrypted with a public key having a corresponding private key that is not generally known.

40. The digital certificate server of claim 35 implemented as an add-on module for use with a conventional digital certificate server.

41. Apparatus for verifying a digitally-signed message, comprising:

(a) input logic for receiving a digitally-signed message and a pseudo-public key allegedly corresponding to a signer of said message;

(b) cryptographic logic for using a public key of an enterprise certifying authority to cryptographically verify the pseudo-public key ; and

(c) signalling logic for detecting fraudulent use of said message upon failure of said verified pseudo-public key to successfully verify said signed message.

42. The apparatus of claim 41 wherein said digitally-signed message is signed using a candidate private key that was generated by a cryptographic key wallet in response to a pseudo-valid access code.

43. The apparatus of claim 42 wherein said key wallet includes:

(a) input logic for receiving a candidate access code;

(b) a first memory configured to store a cryptographically camouflaged access-controlled datum;

(c) first cryptographic logic operatively connected to said input logic and said first memory for processing said cryptographically camouflaged access-controlled datum using said candidate access code; and

(d) output logic for providing said processed datum access-controlled datum to a user of said apparatus.

44. The apparatus of claim 41 wherein said logic for detecting said fraudulent use includes logic for freezing access to said apparatus upon a plurality of unsuccessful attempted verifications.

45. The apparatus of claim 41 wherein said logic for detecting said fraudulent use includes logic for effecting an alarm upon unsuccessful attempted verification.

46. The apparatus of claim 41 wherein said cryptographic logic for using a public key of an enterprise certifying authority to verify the pseudo-public key includes cryptographic logic for decrypting said pseudo-public key.

47. The apparatus of claim 41 wherein said received pseudo-public key is contained in a pseudo-public certificate.

48. A method for providing a stored cryptographically-secured access-controlled datum, comprising the steps of:

(a) receiving a candidate access code from a user of a digital wallet;

(b) accessing a stored, cryptographically camoflagued access-controlled datum;

(c) cryptographically processing said cryptographically camoflagued access-controlled datum using said candidate access code; and

(d) providing said processed datum access-controlled datum to said user of said wallet.

49. The method of claim 48 wherein said step of cryptographically processing said cryptographically camoflaged access-controlled datum using said candidate access code includes:

(a) accessing from a first memory within a digital wallet, an access-controlled datum that has been at least partially encrypted using an access code;

(b) accessing from a second memory within said digital wallet, a cryptographic representation of said access code;

(c) regenerating said cryptographic representation of said access code in response to said candidate access code belonging to a plurality of pseudo-valid access codes; and

(d) using said received candidate access code, decrypting said encrypted access-controlled datum to produce a decrypted access-controlled datum.

50. The method of claim 49 wherein said access-controlled datum is a cryptographic key.

51. The method of claim 50 wherein said cryptographic key is a private key.

52. The method of claim 51 wherein said private key is a member of a cryptographic key pair including a pseudo-public key corresponding to said private key.

53. The method of claim 52 wherein said digital wallet includes a pseudo-public certificate containing said pseudo-public key.

54. The method of claim 53 wherein said pseudo-public key is encrypted.

55. The method of claim 54 wherein said pseudo-public key is encrypted with a public key having a corresponding private key that is not generally known.

56. The method of claim 52 wherein said private key is well-formed.

57. The method of claim 56 wherein said private key includes a modulus not having any small factors, and an exponent smaller than said modulus.

58. The method of claim 56 wherein said private key includes:

(a) a cleartext representation of said modulus; and

(b) a cryptographic representation of at least a part of an exponent corresponding to said modulus.

59. The method of claim 58 wherein:

(a) said private key is stored in said first memory as an expanded form of at least part of said exponent; and

(b) said step of decrypting said encrypted access-controlled datum includes:

(i) retrieving from a third memory a number larger than said exponent and smaller than said modulus;

(ii) retrieving said expanded form of at least part of said exponent from said first memory; and

(iii) evaluating said expanded form of at least part of said exponent, modulo said number, to recover said at least part of said exponent.

60. The method of claim 58 wherein said at least part of said exponent represents certain less significant bits of said exponent.

61. The method of claim 51 wherein said step of regenerating said cryptographic representation of said access code includes performing a many-to-one hash.

62. The method of claim 61 wherein said many-to-one hash is a good hash.

63. The method of claim 50 wherein:

(a) said cryptographic representation includes a hash function; and

(b) said step of regenerating said cryptographic representation of said access code includes performing a many-to-one hash.

64. The method of claim 63 wherein said many-to-one hash is a good hash.

65. The method of claim 64 wherein said good hash is characterized in that said plurality of pseudo-valid access codes are distributed substantially uniformly among a plurality of invalid access codes.

66. The method of claim 63 wherein said access-controlled datum is a private key.

67. The method of claim 66 wherein said private key is a member of a cryptographic key pair including a pseudo-public key corresponding to said private key.

68. The method of claim 66 wherein said private key is well-formed.

69. The method of claim 66 further comprising the steps of:

(a) receiving a message to be signed;

(b) generating random data;

(c) padding said received message with said generated random data; and

(d) signing said padded message with said decrypted access-controlled datum.

70. The method of claim 50 wherein said step of decrypting said access-controlled datum is disallowed when said received candidate access code is an invalid access code.

71. The method of claim 50 implemented as a software program.

72. The method of claim 50 implemented via a hardware device.

73. The method of claim 50 further comprising the steps of:

(a) receiving a message to be signed;

(b) generating random data;

(c) padding said received message with said generated random data; and

(d) signing said padded message with said decrypted access-controlled datum.

74. The method of claim 73 wherein said generated random data is strongly random.

75. The method of claim 74 wherein said generated random data originates from a physical source.

76. The method of claim 50 wherein said step of decrypting said encrypted access-controlled datum includes performing a symmetric cryptographic operation thereon.

77. The method of claim 76 wherein said symmetric cryptographic operation is DES.

78. The method of claim 50 wherein said stored access-controlled datum is a private key having a corresponding public key that includes a long exponent.

79. A method for providing a stored cryptographically-secured access-controlled datum, comprising the steps of:

(a) receiving, at a digital wallet, a user-inputted access code that may belong to a plurality of pseudo-valid access codes;

(b) decrypting, at said digital wallet, a stored access-controlled datum, using said pseudo-valid access code, upon cryptographically verifying said pseudo-valid access code; and

(c) providing said decrypted access-controlled datum to said user of said digital wallet.

80. The method of claim 79 wherein said access-controlled datum includes a private key having a corresponding pseudo-public key.

81. The method of claim 80 wherein said digital wallet includes a pseudo-public certificate containing said pseudo-public key.

82. A method for generating a pseudo-public digital certificate comprising the steps of:

(a) receiving from a requestor a digitally signed request for a pseudo-public digital certificate, said request including:

(i) a pseudo-public key to be certified, and

(ii) an identifying attribute of said requestor;

(b) cryptographically verifying said digitally signed request using said pseudo-public key;

(c) creating said pseudo-public certificate upon said verifying said digitally signed request, said certificate including a cryptographic representation of said pseudo-public key; and

(d) outputting said pseudo-public certificate for said requestor.

83. The method of claim 82 further comprising the step of placing said created digital certificate in a digital wallet, said digital wallet comprising:

(a) input logic for receiving a candidate access code;

(b) a first memory configured to store a cryptographically camouflaged access-controlled datum;

(c) first cryptographic logic operatively connected to said input logic and said first memory for processing said cryptographically camouflaged access-controlled datum using said candidate access code; and

(d) output logic for providing said processed datum access-controlled datum to a user of said apparatus.

84. The method of claim 82 wherein said pseudo-public certificate is of a modified conventional format.

85. The apparatus of claim 84 wherein said pseudo-public key is encrypted.

86. The method of claim 85 wherein:

(a) said pseudo-public key is encrypted with a public key having a corresponding private key that is not generally known.

87. The method of claim 82 performed via an add-on module for use with a conventional digital certificate server.

88. A method for verifying a digitally-signed message, comprising the steps of:

(a) receiving, at a message verification apparatus, a digitally-signed message and a pseudo-public key allegedly corresponding to a signer of said message;

(b) using a public key of an enterprise certifying authority to cryptographically verify the pseudo-public key; and

(c) detecting fraudulent use of said message upon failure of said verified pseudo-public key to successfully verify said signed message.

89. The method of claim 88 wherein said digitally-signed message is signed using a candidate private key that was generated by a cryptographic key wallet in response to a pseudo-valid access code.

90. The method of claim 89 wherein said key wallet includes:

(a) input logic for receiving a candidate access code;

(b) a first memory configured to store a cryptographically camouflaged access-controlled datum;

(c) first cryptographic logic operatively connected to said input logic and said first memory for processing said cryptographically camouflaged access-controlled datum using said candidate access code; and

(d) output logic for providing said processed datum access-controlled datum to a user of said apparatus.

91. The method of claim 88 wherein said step of detecting said fraudulent use includes freezing access to said message verification apparatus upon a plurality of unsuccessful attempted verifications.

92. The method of claim 88 wherein said step of detecting said fraudulent use includes effecting an alarm upon unsuccessful attempted verification.

93. The method of claim 88 wherein said step of using a public key of an enterprise certifying authority to cryptographically verify the pseudo-public key includes decrypting said pseudo-public key.

94. The apparatus of claim 88 wherein said received pseudo-public key is contained in a pseudo-public certificate.

95. A method for storing a stored cryptographically-secured access-controlled datum, comprising the steps of:

(a) receiving an access-controlled datum;

(b) cryptographically camoflaguing said access-controlled datum such to be recognizable by an authorized user thereof but unrecognizable to an unauthorized user thereof; and

(c) storing said camoflaged access-controlled datum in a digital wallet.

96. The method of claim 95 wherein said step of cryptographically camoflaguing said access-controlled datum includes:

(a) receiving an access code;

(b) computing a cryptographic representation of said access code, said representation having the property of being reproducible in response to a plurality of pseudo-valid access codes;

(c) storing said computed cryptographic representation of said access code;

(d) at least partially encrypting said access-controlled datum using said access code;

(e) storing said at least partially encrypted access-controlled datum for subsequent access by a user providing one of said plurality of said pseudo-valid access codes.

97. The method of claim 96 wherein said access-controlled datum is a cryptographic key.